Amendments to the Specification

Please replace paragraph [0026] with the following amended paragraph:

[0026] Similarly, security process 102 may determine whether data element 103 has been compromised by determining whether the data element has been modified by an unauthorized individual or process. There are a number of ways that security process 102 can determine whether ~~code 104~~ data element 103 has been modified unauthorizedly. For example, it could determine whether the ~~code 104~~ data element 103 matches a checksum associated with the data element 103.

Please replace paragraph [0031] with the following amended paragraph:

[0031] The hard, real-time feature of ~~sp102~~ security process 102 is important in situations where application code 104 when executed periodically performs an important task and the consequences of it not performing this important task in an intended manner could be dire. Thus, security process 102, which has the ability to shut down code 104 before it is scheduled to perform the important task when there is an indication that code 104 has been tampered with, is highly valued.

Please replace paragraph [0032] with the following amended paragraph:

[0032] As a specific example, assume that code 104 is configured to output a pre-determined signal at time t=1, t=2, etc. In this example, security process 102 can be configured to check the integrity of code 104 just before code 104 is scheduled to output the signal (e.g., ~~sp102~~ security process 102 can be configured to check the code's integrity at time t=0.9, t=1.9, t=2.9, …). In this manner, if an intruder manages to tamper with code 104 the consequences can be minimized because ~~sp102~~ security process 102 will detect, in the vast majority of cases, the tampering prior to the tampered with code 104 performing its task, and, thus, be able take some form of corrective action before the tampered with code 104 is scheduled to perform its task.

Please replace paragraph [0033] with the following amended paragraph:

[0033] FIG. 3 illustrates a computer system 300 according to another embodiment of the invention. System 300 is similar to the system shown in FIG. 1, with the exception that system 300 further includes [[a]] an external monitor 302 that can be configured to issue challenges to a challenge handler 304, which can be configured to respond to the challenges issued by monitor 302. Although challenge handler is shown as being a separate process from security process 102, this is not a limitation, as the challenge handler may be implemented as part of security process 102.

Please replace paragraph [0035] with the following amended paragraph:

[0035] If the external monitor 302 does not receive a correct response from the challenge handler 304 [[t]] at the appropriate time (e.g., within a specified hard time limit or at the time specified in the challenge), then external monitor 302 may declare that system 300 has been compromised. Thus, to produce an undetected compromise an attacker must not only defeat internal security, but also take over the operation of the challenge handler component 304 before expiration of the hard time limit imposed by the monitor 302.